ADDITIONAL FERMILAB TERMS AND CONDITIONS

FOR SUBCONTRACTS INVOLVING

PERSONALLY IDENTIFIABLE INFORMATION

1. DEFINITIONS

1.1 As used throughout this subcontract, the term "Personally Identifiable Information" shall mean any information collected or maintained by Fermilab, on behalf of the Department of Energy, about an individual, including but not limited to, education, financial transactions, medical history and criminal or employment history, and information that can be used to distinguish or trace an individual's identity, such as his/her name, Social Security number, date and place of birth, mother's maiden name, biometric data, and including any other personal information that is linked or linkable to a specific individual.

2. GENERAL REQUIREMENTS

2.1 Subcontractor must ensure compliance with privacy requirements, specifically those provided in the Privacy Act of 1974, as amended at Title 5 United States Code (U.S.C.) 552a, and take appropriate actions to assist Fermilab in complying with Section 208 of the E-Government Act of 2002, and Office of Management and Budget (OMB)directives.

2.2 Subcontractor must ensure that its employees are aware of their responsibility for safeguarding Personally Identifiable Information (PII) and complying with the Privacy Act.

3. SPECIFIC REQUIREMENTS

3.1 Subcontractor must ensure its employees are made aware of their roles and responsibilities for reporting suspected or confirmed incidents involving the breach of PII

3.2 Subcontractor must ensure its employees are cognizant of the following DOE Privacy Rules of Conduct. At a minimum, Subcontractor must ensure that its employees—(1) are trained in their responsibilities regarding the safeguarding of PII; (2) do not disclose any PII contained in any SOR except as authorized; (3) report any known or suspected loss of control or unauthorized disclosure of PII; (4) observe the requirements of DOE directives concerning marking and safeguarding sensitive information, including, when applicable, DOE O 471.3, *Protecting and Identifying Official Use Only Information*; (5) collect only the minimum PII necessary for the proper performance of a documented agency function; (6) do not place PII on shared drives, intranets or websites without permission of the System Owner; and (7) challenge anyone who asks to see the PII for which they are responsible.

3.3 Subcontractor must ensure that its employees complete the Annual Privacy Training and sign the completion certificate acknowledging their responsibility for maintaining and protecting Privacy Act information prior to being authorized access to all information systems.

3.4 Subcontractor must ensure that its employees are cognizant of the fact that all personal information collected, maintained, used, or disseminated on behalf of the Agency must be maintained in a Privacy Act SOR.

3.5 Subcontractor must ensure that its employees recognize differences between PII and the Privacy Act and the different obligations created by both authorities. Most personal information about an individual will fall under both the Privacy Act and OMB directives governing the safeguarding of PII. However, contractors must be cognizant that these are two separate authorities that impose different responsibilities on federal and contractor employees for safeguarding information. PII that is in a SOR is subject to the restrictions and penalties of the Privacy Act.

3.6 Subcontractor must ensure that its employees are cognizant of the fact that non-compliance with the Privacy Act carries criminal and civil penalties.

4. MANDATORY FLOWDOWN

4.1 Subcontractor is responsible for flowing down the requirements of this FL-300 to sub-subcontractors at any tier to the extent necessary to ensure the Subcontractor's or sub-subcontractor's compliance with the requirements.